REMARKS

Prior to entry of this paper, Claims 1-20 were pending. Claim 1-20 were rejected. In this paper, Claim 1, 12, 18, and 20 are amended; no claims are canceled, or added. Claims 1-20 are currently pending. No new matter is added by way of this amendment. For at least the following reasons, Applicants respectfully submit that each of the presently pending claims is in condition for allowance.

Claim Rejections

In the Advisory Action, the rejections appear to be maintained that claims 1-3, 5-8, 10, and 11 are rejected under 35 USC 102(e) as being anticipated by Benaloh et al., U.S. Patent No. 7,065,216. Claims 4, 9, 12-20 are rejected under 35 USC 103(a) as being unpatentable over Benaloh in view of Cooper et al., US PGPUB No. 20010051996 (hereinafter Cooper). Applicants respectfully traverse these rejections.

For example, claim 1 recites, in part, a method for tracing content by receiving the content from a first entity, decrypting the received content by a second entity that received the content from the first entity, modifying the decrypted content by the second entity by embedding at least one or a fingerprint or watermarked into the decrypted content, and encrypting the modified content by the second entity. The Applicants submit that none of the cited references alone or in combination teach or even suggest such limitations.

Benaloh's watermark or fingerprints do not uniquely identify the second market participant that received the content, decrypted the content, and then embedded the watermark or fingerprint into the decrypted content. Instead, it is the unique public/private key pair that uniquely identifies for Benaloh the content recipient, and then only through the relationship of the keys to the marked content is there a mechanism to identify the recipient of the already watermarked content.

As discussed in prior responses and during an interview with the Examiner, Benaloh describes each of individual partitions of content being separately and uniquely marked, as by any

suitable fingerprinting or watermarking technique. See Benaloh's Figure 9, and Col. 9 lines 2-19. Individual different keys are then associated with each of the uniquely marked partitions. These keys are utilized to encrypt the partitions to provide respective partitions. See Benaloh's Figure 9, and Col. 9 lines 45-60. Next, individual unique key collections are defined which, in any one key collection, there appears one and only one key for one partition or clip in each partition set. See Benaloh's Figure 9, and Col. 9 lines 61-67. Each unique key collection is then associated with a corresponding content player and encrypted with that content player's public device key...only the content player with the corresponding private device key can decrypt the encrypted key collection to access the encrypted content. See Benaloh, Col. 10 lines 4-19. Thus, it is not the watermarks that uniquely identify the entity that decrypted the content and then modified the decrypted content by embedding the fingerprint or watermark, as is required to satisfy at least claim 1. Instead, it is actually the relationship of the public/private keys to the marked content that enables Benaloh to identify the recipient of the already marked content.

Moreover, as clearly discussed during an interview with the Examiner and in prior office actions, the watermarking of the content is not performed in Benaloh by the recipient of the content (the second market participant), but instead appears to be watermarked or fingerprinted by an entity that subsequently delivers the content to each player. See Benaloh's Figures 2 and 12 (block 1216). Thus, Benaloh does not teach or even suggest that the content is received from a first entity, decrypted by a second entity, and modified by the second entity that decrypted the content. Benaloh teaches two different entities: one that performs the watermarking, and a different entity that receives the already marked content and decrypts it. Moreover, there is not even a suggestion that Benaloh enables the recipient of the content to decrypt it, and then modify it with its own unique identifier as would be required by at least claim 1. Thus, Benaloh fails to anticipate or render obvious at least claim 1.

Cooper similarly fails also to teach such limitations. Instead, Cooper also teaches watermarking the content and then transferring (downloading) that content to the user. See Cooper Figure 3. Thus, Cooper teaches that the content is sent to the user as already watermarked content and provides no suggestion otherwise. While Cooper does mention that a media content physical

copy may have two or more watermarks within the content, there is absolutely no teaching or suggestion that such watermarks are embedded by the entity that decrypted the content, as is required by at least claim 1. Instead, Cooper merely points out that an example of using multiple watermarks include one serial number being the master serial number and a second serial number being the physical copy serial number. Cooper also teaches that another embodiment may include adding three watermarks to the downloaded content, including a copyright mark being watermarked into the digital content along with the digital certificate number for the user downloading the content, as well as the ID number for the customer site 270, for example a content source or content distributor. See Cooper, paragraph 0249. The watermarks are not embedded by the entity that decrypted the content, but is instead already watermarked before it is received and then decrypted. Therefore, Cooper fails to teach or even suggest that the content is received from a first entity, decrypted by the second entity, modified by the second entity by embedding the fingerprint or watermark, and then encrypting the modified content by the second entity. Because, Cooper also fails to teach or suggest each of the limitations of at least claim 1, the combination of Benaloh with Cooper also fails to satisfy a *prima facie* case of obviousness. Thus, the Applicants submit that at least claim 1 should be allowed to issue.

Because independent claims 12, 18, and 20 include similar, albeit different, limitations to claim 1, Applicants submit that the cited prior art references either alone or in combination, also fail to anticipate or render obvious these claims as well. For example, claim 12 recites, in part, a security device that receives and decrypted encrypted content, determines a self-identifier for the security device, generates a fingerprint from the self-identifier, and watermarks the content employing the self-identifier. Claim 18 recites, inter alia, a network device that receives a first wrapper of content from a first market participant that is sent to a second market participant that is associated with the network device, decrypts the content at the network device of the second market participant, and embeds a fingerprint or watermark that uniquely identifies the second market participant into the decrypted content at the network device of the second market participant. Again, Benaloh and Cooper, alone or in combination merely teaches that the watermarking or fingerprinting of the content is performed by an entity different from the entity that received the

encrypted content, decrypted the content, and modified the content. Thus, for at least this reason, Benaloh and Cooper, alone or in combination fails to render obvious independent claims 12, 18, and 20 as well. Thus, Applicants request that claims 1, 12, 18, and 20 be allowed to issue.

Moreover, Claim 7, which depends from Claim 1 further recites providing the wrapped modified content to a downstream market recipient, decrypting the received content by the downstream market recipient, and further modifying the decrypted modified content by embedding another fingerprint or watermark into the modified content...that uniquely identifies the downstream market recipient that decrypts the modified content. As is clear, the combination of Claims 1 and 7 result in multiple decrypting and multiple watermarking of the content, each watermarking being performed by that which has decrypted the content and where the watermark uniquely identifies who decrypted the content. Such multiple entities doing such actions are clearly not taught nor suggested by Benaloh. Thus, for at least these reasons, Claim 7 is also allowable.

Moreover, claims 2-11, 13-17, and 19 depend from claims 1, 12, and 18, respectively. Therefore, they are also allowable for at least the same reasons as claims 1, 12, 18, and 20. The Applicants thus respectfully request that these claims also be allowed to issue.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-20) is in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicants reserve the right to raise these arguments in the future.

Dated: March 12, 2008

Respectfully submitted,

By _____
Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(206) 262-8915
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant